CLAIM AMENDMENTS

1.   1.   (Original) A method for facilitating secure communications among multicast nodes

2.   in a telecommunications network, the method comprising the computer-implemented

3.   steps of:

4.   receiving, from a first node, a first request to store an encryption key, wherein the first

5.   request includes an identifier, and wherein the first node uses the encryption

6.   key to encrypt data that is multicast with the identifier to a plurality of second

7.   nodes;

8.   in response to the first request,

9.   storing the encryption key;

10.   creating and storing an association between the encryption key and the

11.   identifier;

12.   receiving, from at least one second node of the plurality of second nodes, a second

13.   request to obtain the encryption key, wherein the second request includes the

14.   identifier;

15.   in response to the second request,

16.   based on the identifier included in the second request and the association

17.   between the encryption key and the identifier, retrieving the encryption

18.   key; and

19.   sending the encryption key to the at least one second node for use in

20.   decrypting the encrypted data.

1.   2.   (Currently Amended) A method as recited in Claim 1, wherein:

2.   a trusted third party performs the steps of receiving the first request, storing the

3.   encryption key, creating and storing the association, receiving the second

4.   request, retrieving the encryption key, and sending the encryption key;

5.   the first request is encrypted based on a first public key that is associated with the

6.   trusted third party;

7.   the first request is signed with a first private key that is associated with the first node;

8.   the first node is a router that acts as a multicast originator; and

9   the plurality of second nodes is a plurality of routers that act as multicast receivers;

10   the trusted third party is selected from the group consisting of a certificate authority, a

11   key distribution center, a key exchange authority, and a key exchange center;

12   the encryption key is selected from the group consisting of a second private key, a

13   shared key, a pseudo-random string of bits, and a pseudo-random string of

14   characters; and

15   the method further comprises the computer-implemented steps of:

16   prior to sending the encryption key,

17   encrypting the encryption key based on a second public key that is

18   associated with the at least one second node; and

19   signing the encrypted encryption key with a third private key that is

20   associated with the trusted third party.

1   3.   (Cancelled)

2   4.   (Cancelled)

1   5.   (Cancelled)

1   6.   (Currently Amended) A method as recited in Claim 5 1, further comprising the

2   computer-implemented steps of:

3   registering a certificate that includes the encryption key and the identifier;

4   in response to the first request, associating an expiration time with the encryption key;

5   in response to the second request, determining based on the expiration time whether

6   the encryption key has expired; and

7   when the encryption key has expired, revoking the certificate.

1   7.   (Cancelled)

1   8.   (Cancelled)

1   9.   (Currently Amended) A method as recited in Claim 1, further comprising the

2   computer-implemented ~~steps~~ step of:

3   generating the encryption key based on an Internet key exchange protocol with the

4   first node.

1   10.   (Cancelled)

1   11.   (Original) A method as recited in Claim 1, wherein:

2   the first node uses the encryption key and Internet protocol security (IPsec) to encrypt

3   the data that is multicast; and

4   the at least one second node decrypts the encrypted data based on the encryption key

5   and IPsec.

1   12.   (Currently Amended) A method as recited in Claim 1, ~~wherein the first request~~

2   ~~includes a list of authorized second nodes, and~~ further comprising the

3   computer-implemented steps of:

4   <u>storing a first list of nodes;</u>

5   <u>in response to the first request, determining whether the first node is included in the</u>

6   <u>first list of nodes;</u>

7   <u>when the first node is included in the first list of nodes, performing the steps of</u>

8   <u>storing the encryption key and creating and storing the association between the</u>

9   <u>encryption key and the identifier;</u>

10   in response to the first request, storing ~~the~~ <u>a second</u> list of ~~authorized second~~ nodes;

11   in response to the second request, determining whether the at least one second node is

12   included in the <u>second</u> list of ~~authorized second~~ nodes; and

13   when the at least one second node is included in the <u>second</u> list of ~~authorized second~~

14   nodes, performing the steps of retrieving and sending the encryption key.

1   13.   (Cancelled)

1 14. (Cancelled)

1 15. (Original) A method as recited in Claim 1, wherein the encryption key is an old
2   encryption key, the identifier is an old identifier, and the association is an old
3   association, and further comprising the steps of:
4   in response to the first request, associating one or more criteria with the encryption
5   key;
6   in response to the second request, determining based on the one or more criteria
7   whether the encryption key is valid; and
8   when the encryption key is not valid,
9   receiving a third request to store a new encryption key, wherein the third
10   request includes a new identifier, and wherein the new encryption key
11   is used to encrypt additional data that is multicast with the new
12   identifier to the plurality of second nodes;
13   in response to the third request,
14   storing the new encryption key;
15   creating and storing a new association between the new encryption key
16   and the new identifier;
17   receiving, from at least one additional second node of the plurality of second
18   nodes, a fourth request to obtain the new encryption key, wherein the
19   fourth request includes the new identifier;
20   in response to the fourth request,
21   based on the new identifier included in the fourth request and the new
22   association between the new encryption key and the new
23   identifier, retrieving the new encryption key; and
24   sending the new encryption key to the at least one additional second
25   node for use in decrypting the encrypted data.

1 16. (Cancelled)

1   17.   (Original) A method as recited in Claim 1,

2   wherein:

3   the identifier is a session identifier;

4   the encrypted data is multicast with an originator identifier that is based on an

5   identity of the first node;

6   the second request includes an unverified originator identifier; and

7   further comprising the computer-implemented steps of:

8   in response to the first request, associating the originator identifier with the

9   session identifier; and

10   in response to the second request, determining whether the unverified

11   originator identifier is valid based on the originator identifier and

12   informing the at least one second node whether the unverified

13   originator is valid.

1   18.   (Cancelled)

1   19.   (Cancelled)

1   20.   (Original) A method as recited in Claim 1, wherein the identifier is selected from the

2   group consisting of a hostname, an Internet protocol address, a media access control

3   address, an Internet security protocol security parameter index, a first string of

4   pseudo-random bits, a second string of pseudo-random characters, a third string of

5   arbitrary bits, and a fourth string of arbitrary characters.

1   21.   (Original) A method for encrypting communications among multicast nodes in a

2   telecommunications network, the method comprising the computer-implemented steps

3   of:

4   sending an encryption key and an identifier that is associated with the encryption key

5   to an authoritative node that stores the encryption key and identifier and that

6   creates and stores an association between the encryption the encryption key

7   and the identifier;

8   encrypting data based on the encryption key; and

9   multicasting the encrypted data with the identifier to one or more receiving nodes,

10   wherein the one or more receiving nodes use the identifier to retrieve the

11   encryption key from the authoritative node and decrypt the encrypted data

12   based on the encryption key.

1   22.   (Previously Presented) A method for decrypting encrypted communications among

2   multicast nodes in a telecommunications network, the method comprising the

3   computer-implemented steps of:

4   receiving from an originating node a multicast that includes encrypted data and an

5   identifier;

6   identifying the identifier from the multicast;

7   sending a request that includes the identifier to an authoritative node for an encryption

8   key used by the originating node to encrypt the encrypted data;

9   in response to the request to the authoritative node, receiving the encryption key; and

10   decrypting the encrypted data based on the encryption key.

7

1   23.   (Original) A method for a certificate authority to facilitate communications based on

2   Internet protocol security (IPsec) among multicast nodes in a telecommunications

3   network, the method comprising the computer-implemented steps of:

4   receiving, at the certificate authority from a first router that acts as a multicast

5   originator, a first request to register an encryption key, wherein the first

6   request includes a multicast session identifier and a list of authorized multicast

7   receivers, and wherein the first router uses the encryption key to encrypt data

8   based on IPsec and multicasts the encrypted data with the multicast session

9   identifier to a plurality of second routers that act as multicast receivers;

10   in response to the first request, the certificate authority creating and storing a

11   multicast session certificate that includes the encryption key, the multicast

12   session identifier, and the list of authorized multicast receivers;

13   receiving, at the certificate authority from at least a particular second router of the

14   plurality of second routers, a second request to obtain the encryption key,

15   wherein the second request includes the multicast session identifier;

16   in response to the second request,

17   determining whether the particular second router is included in the list of

18   authorized multicast receivers;

19   when the particular second router is included in the list of authorized multicast

20   receivers,

21   based on the multicast session identifier included in the second request

22   and the multicast session certificate, the certificate authority

23   retrieving the encryption key; and

24   the certificate authority sending the encryption key to the particular

25   second router for use in decrypting the encrypted data based on

26   IPsec.

1   24.   (Previously Presented) A computer-readable medium carrying one or more sequences

2   of instructions for facilitating secure communications among multicast nodes in a

3   telecommunications network, which instructions, when executed by one or more

4   processors, cause the one or more processors to carry out the steps of:

5   receiving, from a first node, a first request to store an encryption key, wherein the first

6   request includes an identifier, and wherein the first node uses the encryption

7   key to encrypt data that is multicast with the identifier to a plurality of second

8   nodes;

9   in response to the first request,

10   storing the encryption key;

11   creating and storing an association between the encryption key and the

12   identifier;

13   receiving, from at least one second node of the plurality of second nodes, a second

14   request to obtain the encryption key, wherein the second request includes the

15   identifier;

16   in response to the second request,

17   based on the identifier included in the second request and the association

18   between the encryption key and the identifier, retrieving the encryption

19   key; and

20   sending the encryption key to the at least one second node for use in

21   decrypting the encrypted data.

1   25.   (Previously Presented) A computer-readable medium carrying one or more sequences

2   of instructions for encrypting communications among multicast nodes in a

3   telecommunications network, cause the one or more processors to carry out the steps

4   of:

5   sending an encryption key and an identifier that is associated with the encryption key

6   to an authoritative node that stores the encryption key and identifier and that

7   creates and stores an association between the encryption the encryption key

8   and the identifier;

9   encrypting data based on the encryption key; and

10   multicasting the encrypted data with the identifier to one or more receiving nodes,

11   wherein the one or more receiving nodes use the identifier to retrieve the

12   encryption key from the authoritative node and decrypt the encrypted data

13   based on the encryption key.

1   26.   (Previously Presented) An apparatus for facilitating secure communications among

2   multicast nodes in a telecommunications network, comprising:

3   means for receiving, from a first node, a first request to store an encryption key,

4   wherein the first request includes an identifier, and wherein the first node uses

5   the encryption key to encrypt data that is multicast with the identifier to a

6   plurality of second nodes;

7   means for storing the encryption key, in response to the first request;

8   means for creating and storing an association between the encryption key and the

9   identifier, in response to the first request;

10   means for receiving, from at least one second node of the plurality of second nodes, a

11   second request to obtain the encryption key, wherein the second request

12   includes the identifier;

13   means for retrieving the encryption key, in response to the second request and based

14   on the identifier included in the second request and the association between

15   the encryption key and the identifier; and

16   means for sending the encryption key to the at least one second node for use in

17   decrypting the encrypted data, in response to the second request.

1   27.   (Previously Presented) An apparatus for encrypting communications among multicast

2   nodes in a telecommunications network, comprising:

3   means for sending an encryption key and an identifier that is associated with the

4   encryption key to an authoritative node that stores the encryption key and

5   identifier and that creates and stores an association between the encryption the

6   encryption key and the identifier;

7   means for encrypting data based on the encryption key; and

8   means for multicasting the encrypted data with the identifier to one or more receiving

9   nodes, wherein the one or more receiving nodes use the identifier to retrieve

10   the encryption key from the authoritative node and decrypt the encrypted data

11   based on the encryption key.

1   28.   (Previously Presented) An apparatus for facilitating secure communications among

2   multicast nodes in a telecommunications network, comprising:

3   a processor;

4   one or more stored sequences of instructions which, when executed by the processor,

5   cause the processor to carry out the steps of:

6   receiving, from a first node, a first request to store an encryption key, wherein

7   the first request includes an identifier, and wherein the first node uses

8   the encryption key to encrypt data that is multicast with the identifier

9   to a plurality of second nodes;

10   in response to the first request,

11   storing the encryption key;

12   creating and storing an association between the encryption key and the

13   identifier;

14   receiving, from at least one second node of the plurality of second nodes, a

15   second request to obtain the encryption key, wherein the second

16   request includes the identifier;

17   in response to the second request,

18   based on the identifier included in the second request and the

19   association between the encryption key and the identifier,

20   retrieving the encryption key; and

21   sending the encryption key to the at least one second node for use in

22   decrypting the encrypted data.

1   29.   (Previously Presented) An apparatus for encrypting communications among multicast

2   nodes in a telecommunications network, comprising:

3   a processor;

4   one or more stored sequences of instructions which, when executed by the processor,

5   cause the processor to carry out the steps of:

6   sending an encryption key and an identifier that is associated with the

7   encryption key to an authoritative node that stores the encryption key

8   and identifier and that creates and stores an association between the

9   encryption the encryption key and the identifier;

10   encrypting data based on the encryption key; and

11   multicasting the encrypted data with the identifier to one or more receiving

12   nodes, wherein the one or more receiving nodes use the identifier to

13   retrieve the encryption key from the authoritative node and decrypt the

14   encrypted data based on the encryption key.

1   30.   (New) An apparatus as recited in Claim 26, wherein:

2   the means for receiving the first request, storing the encryption key, creating and

3   storing the association, receiving the second request, retrieving the encryption

4   key, and sending the encryption key are included in a trusted third party;

5   the first request is encrypted based on a first public key that is associated with the

6   trusted third party;

7   the first request is signed with a first private key that is associated with the first node;

8   the first node is a router that acts as a multicast originator;

9   the plurality of second nodes is a plurality of routers that act as multicast receivers;

10   the trusted third party is selected from the group consisting of a certificate authority, a

11   key distribution center, a key exchange authority, and a key exchange center;

12   the encryption key is selected from the group consisting of a second private key, a

13   shared key, a pseudo-random string of bits, and a pseudo-random string of

14   characters; and

15   the apparatus further comprises:

16   means for encrypting, prior to sending the encryption key, the encryption key

17   based on a second public key that is associated with the at least one

18   second node; and

19   means for signing, prior to sending the encryption key, the encrypted

20   encryption key with a third private key that is associated with the

21   trusted third party.

1   31.   (New) An apparatus as recited in Claim 26, further comprising:

2   means for registering a certificate that includes the encryption key and the identifier;

3   means for associating, in response to the first request, an expiration time with the

4   encryption key;

5   means for determining, in response to the second request, based on the expiration

6   time whether the encryption key has expired; and

7   means for revoking the certificate when the encryption key has expired.

1   32.   (New) An apparatus as recited in Claim 26, further comprising:

2   means for generating the encryption key based on an Internet key exchange protocol

3   with the first node.

1   33.   (New) An apparatus as recited in Claim 26, wherein:

2   the first node uses the encryption key and Internet protocol security (IPsec) to encrypt

3   the data that is multicast; and

4   the at least one second node decrypts the encrypted data based on the encryption key

5   and IPsec.

1   34.   (New) An apparatus as recited in Claim 26, further comprising:

2   means for storing a first list of nodes;

3   means for determining, in response to the first request, whether the first node is

4   included in the first list of nodes;

5   means for causing, when the first node is included in the first list of nodes, the storing

6   of the encryption key and the creating and storing of the association between

7   the encryption key and the identifier;

8   means for storing, in response to the first request, a second list of nodes;

9   means for determining, in response to the second request, whether the at least one

10   second node is included in the second list of nodes; and

11   means for causing, when the at least one second node is included in the second list of

12   nodes, the retrieving and sending of the encryption key.

1 35. (New) An apparatus as recited in Claim 26, wherein the encryption key is an old

2   encryption key, the identifier is an old identifier, and the association is an old

3   association, and further comprising:

4   means for associating, in response to the first request, one or more criteria with the

5   encryption key;

6   means for determining, in response to the second request, based on the one or more

7   criteria whether the encryption key is valid;

8   means for receiving, when the encryption key is not valid, a third request to store a

9   new encryption key, wherein the third request includes a new identifier, and

10   wherein the new encryption key is used to encrypt additional data that is

11   multicast with the new identifier to the plurality of second nodes;

12   means for storing, in response to the third request, the new encryption key;

13   means for creating and storing, in response to the third request, a new association

14   between the new encryption key and the new identifier;

15   means for receiving, from at least one additional second node of the plurality of

16   second nodes, a fourth request to obtain the new encryption key, wherein the

17   fourth request includes the new identifier;

18   means for retrieving, in response to the fourth request, the new encryption key, based

19   on the new identifier included in the fourth request and the new association

20   between the new encryption key and the new identifier; and

21   means for sending, in response to the fourth request, the new encryption key to the at

22   least one additional second node for use in decrypting the encrypted data.

1   36.   (New) An apparatus as recited in Claim 26,

2   wherein:

3   the identifier is a session identifier;

4   the encrypted data is multicast with an originator identifier that is based on an

5   identity of the first node;

6   the second request includes an unverified originator identifier; and

7   further comprising:

8   means for associating, in response to the first request, the originator identifier

9   with the session identifier; and

10   means for determining, in response to the second request, whether the

11   unverified originator identifier is valid based on the originator

12   identifier and informing the at least one second node whether the

13   unverified originator is valid.

1   37.   (New) An apparatus as recited in Claim 26, wherein the identifier is selected from the

2   group consisting of a hostname, an Internet protocol address, a media access control

3   address, an Internet security protocol security parameter index, a first string of

4   pseudo-random bits, a second string of pseudo-random characters, a third string of

5   arbitrary bits, and a fourth string of arbitrary characters.

1   38.   (New) An apparatus as recited in Claim 28, wherein:

2   the apparatus is part of a trusted third party;

3   the first request is encrypted based on a first public key that is associated with the

4   trusted third party;

5   the first request is signed with a first private key that is associated with the first node;

6   the first node is a router that acts as a multicast originator;

7   the plurality of second nodes is a plurality of routers that act as multicast receivers;

8   the trusted third party is selected from the group consisting of a certificate authority, a

9   key distribution center, a key exchange authority, and a key exchange center;

10   the encryption key is selected from the group consisting of a second private key, a

11   shared key, a pseudo-random string of bits, and a pseudo-random string of

12   characters; and

13   the apparatus further comprises one or more stored sequences of instructions which,

14   when executed by the processor, cause the processor to carry out the steps of:

15   prior to sending the encryption key,

16   encrypting the encryption key based on a second public key that is

17   associated with the at least one second node; and

18   signing the encrypted encryption key with a third private key that is

19   associated with the trusted third party.

1   39.   (New) An apparatus as recited in Claim 28, further comprising one or more stored

2   sequences of instructions which, when executed by the processor, cause the processor

3   to carry out the steps of:

4   registering a certificate that includes the encryption key and the identifier;

5   in response to the first request, associating an expiration time with the encryption key;

6   in response to the second request, determining based on the expiration time whether

7   the encryption key has expired; and

8   when the encryption key has expired, revoking the certificate.

1   40.   (New) An apparatus as recited in Claim 28, further comprising one or more stored

2   sequences of instructions which, when executed by the processor, cause the processor

3   to carry out the step of:

4   generating the encryption key based on an Internet key exchange protocol with the

5   first node.

1   41.   (New) An apparatus as recited in Claim 28, wherein:

2   the first node uses the encryption key and Internet protocol security (IPsec) to encrypt

3   the data that is multicast; and

4   the at least one second node decrypts the encrypted data based on the encryption key

5   and IPsec.

1   42.   (New) An apparatus as recited in Claim 28, further comprising one or more stored

2   sequences of instructions which, when executed by the processor, cause the processor

3   to carry out the steps of:

4   storing a first list of nodes;

5   in response to the first request, determining whether the first node is included in the

6   first list of nodes;

7   when the first node is included in the first list of nodes, performing the steps of

8   storing the encryption key and creating and storing the association between the

9   encryption key and the identifier;

10   in response to the first request, storing a second list of nodes;

11   in response to the second request, determining whether the at least one second node is

12   included in the second list of nodes; and

13   when the at least one second node is included in the second list of nodes, performing

14   the steps of retrieving and sending the encryption key.

1   43.   (New) An apparatus as recited in Claim 28, wherein the encryption key is an old

2   encryption key, the identifier is an old identifier, and the association is an old

3   association, and further comprising one or more stored sequences of instructions

4   which, when executed by the processor, cause the processor to carry out the steps of:

5   in response to the first request, associating one or more criteria with the encryption

6   key;

7   in response to the second request, determining based on the one or more criteria

8   whether the encryption key is valid; and

9   when the encryption key is not valid,

10   receiving a third request to store a new encryption key, wherein the third

11   request includes a new identifier, and wherein the new encryption key

12   is used to encrypt additional data that is multicast with the new

13   identifier to the plurality of second nodes;

14   in response to the third request,

15   storing the new encryption key;

17

16   creating and storing a new association between the new encryption key

17   and the new identifier;

18   receiving, from at least one additional second node of the plurality of second

19   nodes, a fourth request to obtain the new encryption key, wherein the

20   fourth request includes the new identifier;

21   in response to the fourth request,

22   based on the new identifier included in the fourth request and the new

23   association between the new encryption key and the new

24   identifier, retrieving the new encryption key; and

25   sending the new encryption key to the at least one additional second

26   node for use in decrypting the encrypted data.

1   44.   (New) An apparatus as recited in Claim 28,

2   wherein:

3   the identifier is a session identifier;

4   the encrypted data is multicast with an originator identifier that is based on an

5   identity of the first node;

6   the second request includes an unverified originator identifier; and

7   further comprising one or more stored sequences of instructions which, when

8   executed by the processor, cause the processor to carry out the steps of:

9   in response to the first request, associating the originator identifier with the

10   session identifier; and

11   in response to the second request, determining whether the unverified

12   originator identifier is valid based on the originator identifier and

13   informing the at least one second node whether the unverified

14   originator is valid.

1   45.   (New) An apparatus as recited in Claim 28, wherein the identifier is selected from the

2   group consisting of a hostname, an Internet protocol address, a media access control

3   address, an Internet security protocol security parameter index, a first string of

4   pseudo-random bits, a second string of pseudo-random characters, a third string of

5   arbitrary bits, and a fourth string of arbitrary characters.

Docket No. 50325-0607 (Seq.No. 1640)